(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－315175
（P2000－315175A）
(43)公開日　平成12年11月14日(2000.11.14)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
G06F 12/14	320	G06F 12/14	320B
9/06	550	9/06	550B
H04L 9/08		H04L 9/00	601D
			601E

審査請求 有　請求項の数9　OL　（全 13 頁）

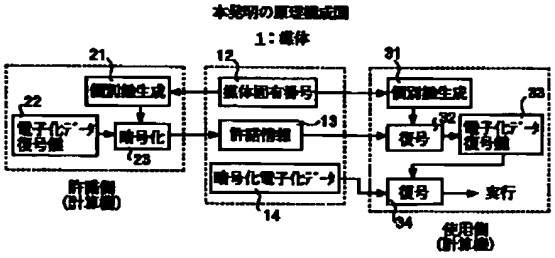
(21)出願番号　特願2000－79015(P2000－79015)
(62)分割の表示　特願平4－58048の分割
(22)出願日　平成４年３月16日(1992.3.16)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　データ書込装置、データ読取装置、記憶媒体および鍵共有方法

(57)【要約】
【目的】　媒体に媒体固有番号を持たせ、媒体固有番号に対してソフトウェアを実行する許諾を与え、正規の媒体に格納され、かつ許諾の与えたソフトウェアだけ実行可能とすること。
【構成】　暗号化電子化データ１４および媒体固有の媒体固有番号１２を格納する媒体１を設け、許諾側で媒体１の媒体固有番号１２をもとに媒体固有鍵を生成し、この媒体固有鍵によって電子化データ復号鍵を暗号化して許諾情報１３とし、使用側で媒体１から読み込んだ媒体固有番号１２をもとに媒体固有鍵を生成し、この媒体固有鍵によって許諾情報１３を復号して電子化データ復号鍵を生成し、電子化データ復号鍵によって読み込んだ暗号化電子化データ１４を復号し、平文の電子化データにするように構成する。



1

【特許請求の範囲】
【請求項１】　暗号化したデータを記憶媒体に書き込むデータ書込装置であって、
前記記憶媒体を一意に特定する媒体固有番号に基づいて前記データを暗号化する暗号化手段と、
前記暗号化手段により暗号化された暗号化データを前記記録媒体に書き込む書込手段と、
を備えたことを特徴とするデータ書込装置。
【請求項２】　前記記憶媒体は、前記暗号化データを読み取るデータ読取装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする請求項１に記載のデータ書込装置。
【請求項３】　各記憶媒体を一意に特定する媒体固有番号と、前記媒体固有番号に基づいて暗号化された暗号化データとを記憶する記憶媒体から前記暗号化データを読み取るデータ読取装置であって、
前記記憶媒体から前記媒体固有番号を読み取る媒体固有番号読取手段と、
前記媒体固有番号読取手段により読み取られた媒体固有番号に基づいて、前記記憶媒体上の暗号化データを復号する復号手段と、
を備えたことを特徴とするデータ読取装置。
【請求項４】　前記記憶媒体は、前記データ読取装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする請求項３に記載のデータ読取装置。
【請求項５】　データ書込装置で書き込まれ、データ読取装置で読み取られるデータを格納した記憶媒体であって、
各記憶媒体を一意に特定する媒体固有番号と、
前記媒体固有番号に基づいて暗号化した暗号化データと、
を格納したことを特徴とする記憶媒体。
【請求項６】　前記データ書込装置によって暗号化データを生成するために使用される媒体固有番号を格納することを特徴とする請求項５に記載の記憶媒体。
【請求項７】　前記データ読取装置によって暗号化データを復号するために使用される媒体固有番号を格納することを特徴とする請求項５に記載の記憶媒体。
【請求項８】　前記データ読取装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする請求項５、６または７に記載の記憶媒体。
【請求項９】　データを暗号化して記憶媒体に書き込むデータ書込装置と前記記憶媒体に格納した暗号化データを復号化するデータ読取装置との間で暗号鍵を共有する鍵共有方法において、
前記記憶媒体に格納された該記憶媒体を一意に特定する媒体固有番号を読み取る読取工程と、
前記読取工程により読み取られた媒体固有番号に基づいて媒体固有鍵を生成する生成工程と、

2

を含んだことを特徴とする鍵共有方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、記憶媒体に格納したコンピュータソフトウエアや電子出版物などの不正使用を防止する電子化データ保護システム、使用許諾者側装置および使用者側装置に関する。
【０００２】ソフトウェアは一般的にコピーが容易である。また、これらの不正コピー行為は、頻繁に行われており、これがソフトウェアベンダーの正当な利益を阻み、その結果、ソフトウェアの価格も高めに設定せざるを得ないといった悪循環が生じている。また、近年の電子出版物が盛んに出版されるようになってきており、著作権の問題は更に重要となり、これらのプログラムやデータの不正コピーを防止することが求められている。
【０００３】
【従来の技術】従来、プログラムや電子出版物、特にソフトウェアを保護する保護方式として、図１４に示すように、ユーザ固有のユーザ固有番号９１を用いて許諾情報７２を生成する方式がある。この従来の方式は、ユーザ固有番号９１として例えば装置番号（計算機に付与された固有の装置番号）を用いる。ソフトウェアは、暗号化してソフトウェア格納媒体７１に格納する。また、許諾情報７２として、ユーザ固有番号９１からユーザの固有鍵を生成し、この固有鍵でソフト復号鍵８２を暗号化して当該許諾情報７２を生成し、ソフトウェア格納媒体７１に格納する。ユーザは、ソフトウェア格納媒体７１に格納された暗号化ソフトウェア７３と許諾情報７２の販売を受けることにより、暗号化ソフトウェア７３を平文のソフトウェアに復号し、これを実行する。以下図１４の従来の構成および動作を簡単に説明する。
【０００４】図１４は、従来技術の説明図を示す。図１４において、ソフトウェア格納媒体７１は、暗号化した暗号化ソフトウェア７３およびソフト復号鍵８２を暗号化した許諾情報７２を格納する媒体、例えば光磁気ディスクであって、ユーザが販売側から購入する対象の媒体である。許諾情報７２は、暗号化ソフトウェア７３を復号して平文のソフトウェアにする情報であって、ソフト復号鍵８２を暗号化したものである。暗号化ソフトウェア７３は、ソフトウェアを暗号化したものである。許諾情報の販売側には、個別鍵生成８１、ソフト復号鍵８２および暗号化回路８３などがある。個別鍵生成８１は、ユーザ計算機のユーザ固有番号（例えば装置番号）９１をもとにユーザ固有の個別鍵を生成するものである。
【０００５】ソフト復号鍵８２は、暗号化ソフトウェア７３を元の平文のソフトウェアに復号するための鍵である。暗号化回路８３は、ソフト復号鍵８２を、個別鍵生成８１によって生成したユーザ固有の個別鍵によって暗号化した許諾情報７２を生成する回路である。また、ユーザ側のユーザ計算機には、ユーザ固有番号９１、個別

鍵生成９２、復号回路９３、ソフト復号鍵９４、および復号回路９５などがある。ユーザ固有番号９１は、ユーザ計算機が持つ固有の番号であって、例えば装置番号である。

【０００６】個別鍵生成９２は、ユーザ固有番号９１をもとに、ユーザ固有の個別鍵を生成するものである。復号回路９３は、購入したソフトウェア格納媒体７１から読み出した許諾情報７２を復号し、ソフト復号鍵９４を生成するものである。ソフト復号鍵９４は、暗号化ソフトウェア７３を復号して平文のソフトウェアに復号するための鍵である。復号回路９５は、ソフト復号鍵９４をもとに、ソフトウェア格納媒体７１から読み出した暗号化ソフトウェア７３を復号し、元の平文のソフトウェアにするものである。この平文のソフトウェアを、ユーザ計算機の主記憶にローディングし、実行する。

【０００７】次に、動作を説明する。

（１）許諾情報の許諾側は、ユーザ計算機の持つユーザ固有番号９１をもとに、個別鍵生成８１がユーザ固有の個別鍵を生成する。この生成した個別鍵をもとに、暗号化回路８３がソフト復号鍵８２を暗号化し、許諾情報７２としてソフトウェアを暗号化した暗号化ソフトウェア７３が格納されたソフトウェア格納媒体７１に書き込む。

【０００８】（２）ユーザは、（１）で許諾情報７２および暗号化ソフトウェア７３の書き込まれたソフトウェア格納媒体７１を購入し、ソフトウェア格納媒体７１をユーザ計算機に装着する。個別鍵生成９２がユーザ計算機の持つ固有のユーザ固有番号（例えば装置番号）９１をもとに、ユーザ固有の個別鍵を生成する。復号回路９３がこの生成したユーザ固有の個別鍵をもとに、購入したソフトウェア格納媒体７１から読み出した許諾情報７２を復号し、ソフト復号鍵９４を生成する。次に、復号回路９５がこの生成したソフト復号鍵９４をもとに、ソフトウェア格納媒体７１から読み出した暗号化ソフトウェア７３を復号し、平文のソフトウェアを生成する。この生成した平文のソフトウェアを主記憶にローディングし、実行する。

【０００９】

【発明が解決しようとする課題】上述した図１４の構成の従来の保護方式は、ユーザ固有番号９１を用いており、通常は計算機の固有番号あるいは携帯可能なハードウェアの固有番号を用いている。計算機の固有番号を用いた場合には、許諾情報７２は、計算機に対して実行の許諾を与えていることとなり、この計算機でしか実行できなくなるため、正当なユーザであっても、異なる計算機上では実行が不可能となるという問題が生じている。また、ソフトウェアの譲渡もできない。

【００１０】また、携帯可能なハードウェアの固有番号を用いた場合には、ハードウェア自体および計算機とのインタフェースを設ける必要があり、実施に伴うコストが増加するために実施が困難になるという問題が生じている。

【００１１】本発明は、これらの問題を解決するため、電子化データの媒体に媒体固有番号を持たせ、この媒体固有番号に対して使用する許諾を与え、正規の媒体に格納され、かつ許諾の与えた電子化データのみ実行可能とすることを目的としている。

【００１２】

【課題を解決するための手段】上記目的を達成するため、請求項１の発明に係るデータ書込装置は、暗号化したデータを記憶媒体に書き込むデータ書込装置であって、前記記憶媒体を一意に特定する媒体固有番号に基づいて前記データを暗号化する暗号化手段と、前記暗号化手段により暗号化された暗号化データを前記記録媒体に書き込む書込手段と、を備えたことを特徴とする。

【００１３】この請求項１の発明によれば、記憶媒体を一意に特定する媒体固有番号に基づいてデータを暗号化し、暗号化した暗号化データを記録媒体に書き込むこととしたので、媒体固有番号に基づく暗号化を伴った暗号化データの書き込みをおこなうことができる。

【００１４】また、請求項２の発明に係るデータ書込装置は、請求項１の発明において、前記記憶媒体は、前記暗号化データを読み取るデータ読取装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする。

【００１５】この請求項２の発明によれば、暗号化データを読み取るデータ読取装置による書き替えが不可能な形式で媒体固有番号を記憶媒体に記憶することとしたので、記憶媒体に記憶した暗号化データを他の記憶媒体に複写する不正使用を防止することができる。

【００１６】また、請求項３の発明に係るデータ読込装置は、各記憶媒体を一意に特定する媒体固有番号と、前記媒体固有番号に基づいて暗号化された暗号化データとを記憶する記憶媒体から前記暗号化データを読み取るデータ読取装置であって、前記記憶媒体から前記媒体固有番号を読み取る媒体固有番号読取手段と、前記媒体固有番号読取手段により読み取られた媒体固有番号に基づいて、前記記憶媒体上の暗号化データを復号する復号手段と、を備えたことを特徴とする。

【００１７】この請求項３の発明によれば、記憶媒体から媒体固有番号を読み取り、読み取った媒体固有番号に基づいて、記憶媒体上の暗号化データを復号することとしたので、正規な記憶媒体に記憶された暗号化データのみを正しく復号化し、もってデータの不正使用を効率良く防止することができる。

【００１８】また、請求項４の発明に係るデータ読取装置は、請求項３の発明において、前記記憶媒体は、前記データ読取装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする。

【００１９】この請求項４の発明によれば、記憶媒体

は、データ読取装置による書き替えが不可能な形式で媒体記憶番号を記憶することとしたので、記憶媒体に記憶した暗号化電子化データを他の記憶媒体に複写する不正使用を防止することができる。

【００２０】また、請求項５の発明に係る記憶媒体は、データ書込装置で書き込まれ、データ読取装置で読み取られるデータを格納した記憶媒体であって、各記憶媒体を一意に特定する媒体固有番号と、前記媒体固有番号に基づいて暗号化した暗号化データと、を格納したことを特徴とする。

【００２１】この請求項５の発明によれば、各記憶媒体を一意に特定する媒体固有番号と、媒体固有番号に基づいて暗号化した暗号化データとを記憶媒体に格納することとしたので、媒体固有番号を利用して暗号化した暗号化データを簡易に授受することができる。

【００２２】また、請求項６の発明に係る記憶媒体は、請求項５の発明において、前記データ書込装置によって暗号化データを生成するために使用される媒体固有番号を格納することを特徴とする。

【００２３】この請求項６の発明によれば、データ書込装置によって暗号化データを生成するために使用される媒体固有番号を格納することとしたので、かかる媒体固有番号を用いて効率良く暗号化することができる。

【００２４】また、請求項７の発明に係る記憶媒体は、請求項５の発明において、前記データ読取装置によって暗号化データを復号するために使用される媒体固有番号を格納することを特徴とする。

【００２５】この請求項７の発明によれば、データ読取装置によって暗号化データを復号するために使用される媒体固有番号を格納することとしたので、かかる媒体固有番号を用いて効率良く復号化することができる。

【００２６】また、請求項８の発明に係る記憶媒体は、請求項５、６または７の発明において、前記データ読取装置による書き替えが不可能な形式で前記媒体固有番号を記憶することを特徴とする。

【００２７】この請求項８の発明によれば、データ読取装置による書き替えが不可能な形式で媒体記憶番号を記憶することとしたので、記憶媒体に記憶した暗号化データを他の記憶媒体に複写する不正使用を防止することができる。

【００２８】また、請求項９の発明に係る鍵共有方法は、データを暗号化して記憶媒体に書き込むデータ書込装置と前記記憶媒体に格納した暗号化データを復号化するデータ読取装置との間で暗号鍵を共有する鍵共有方法において、前記記憶媒体に格納された該記憶媒体を一意に特定する媒体固有番号を読み取る読取工程と、前記読取工程により読み取られた媒体固有番号に基づいて媒体固有鍵を生成する生成工程と、を含んだことを特徴とする。

【００２９】この請求項９の発明によれば、記憶媒体に格納された該記憶媒体を一意に特定する媒体固有番号を読み取り、読み取った媒体固有番号に基づいて媒体固有鍵を生成することとしたので、データ書込装置とデータ読取装置が容易に鍵を共有化することができる。

【００３０】具体的には、図１は、本発明の原理構成図を示す図であり、図１において、媒体１は、暗号化した暗号化電子化データ１４、当該媒体固有の一意の媒体固有番号１２および許諾情報１３を格納するものである。

【００３１】個別鍵生成２１、３１は、媒体固有番号１２から媒体個別鍵を生成するものである。暗号化２３は、媒体個別鍵によって電子化データ復号鍵２２を暗号化するものである。復号３２は、媒体個別鍵によって許諾情報１３を復号して電子化データ復号鍵３３を生成するものである。復号３４は、電子化データ復号鍵３３によって暗号化電子化データ１４を復号し、平文の電子化データを生成するものである。

【００３２】本発明は、図１に示すように、媒体１に予め一意の媒体固有番号１２と共に暗号化した暗号化電子化データ１４を書き込んでおき、許諾側で個別鍵生成２１が媒体１の一意の媒体固有番号１２をもとに媒体固有鍵を生成し、暗号化２３がこの媒体固有鍵によって電子化データ復号鍵２２を暗号化し、使用側で個別鍵生成３１が媒体１から読み込んだ媒体固有番号１２をもとに媒体固有鍵を生成し、復号３２が受信した許諾情報１３を媒体固有鍵によって復号して元の電子化データ復号鍵３３を生成し、復号３４がこの電子化データ復号鍵３３によって読み込んだ暗号化電子化データ１４を復号し、平文の電子化データにするようにしている。このため、かかる許諾側と使用側では、媒体固有番号１２に基づく媒体固有鍵を共有できることになる。

【００３３】また、１つの媒体１に格納する暗号化電子化データ１４毎に異なる電子化データ復号鍵２２を対応づけ、許諾側で使用を許可する暗号化電子化データ１４の電子化データ復号鍵２２のみを媒体固有鍵によってそれぞれ暗号化して許諾情報１３とし、使用側で受信した許諾情報１３に対応する暗号化電子化データ１４のみを復号し、平文の電子化データにするようにしている。

【００３４】また、媒体固有の一意の媒体固有番号１２を使用側で書き替え不可能な形態で書き込むようにしている。また、暗号化電子化データ１４として、計算機を動作させるソウトウェアあるいは各種データ（文字、画像、音声データなど）を暗号化するようにしている。

【００３５】また、暗号化電子化データ１４を格納する媒体１に一意の媒体固有番号１２を書き替え不可能な形態で持たせ、この媒体固有番号１２に対して電子化データを使用する許諾を与えることにより、正規の媒体１に格納され、かつ許諾の与えた暗号化電子化データ１４のみの使用を可能とすることができると共に、媒体１に格納されている電子化データの譲渡を可能とし、別の電子計算機に当該媒体１を装填して使用することができる。

【００３６】
【発明の実施の形態】次に、図２から図１３を用いて本発明の実施例の構成および動作を詳細に説明する。ここで、図１で説明した電子化データの例として、計算機に使用するソフトウェアを例に以下説明する。
【００３７】図２は、本発明の１実施例構成図を示す。図２において、ソフトウェア格納媒体１１は、許諾側が使用側に許諾するソフトウェアを格納する媒体であり、例えば光磁気ディスク（数百Mバイトないし数Gバイトの容量を持つディスク）などの媒体である。このソフトウェア格納媒体１１には、図示のように、書き替え不可な媒体固有番号１２、使用側にソフトウェアの許諾を与える許諾情報１３、およびソフトウェアを暗号化した暗号化ソフトウェア１５を格納する。
【００３８】媒体固有番号１２は、ソフトウェア格納媒体１１に書き替え不可な一意な媒体固有の番号である。この媒体固有番号１２は、ユーザが書き替え不可能な領域に書き込み、ＯＳが管理するようにしてもよいし、また、ＯＳといえども書き替え不可能な形で予め書き込んだり、一度書き込んだら修正不可のものでもよい。
【００３９】許諾情報１３は、許諾側が使用側にソフトウェアの許諾を与える情報であって、ここでは、暗号化ソフトウェア１５を復号する暗号データである（図６、図７を用いて詳述する）。
【００４０】暗号化ソフトウェア１５は、ソフトウェアを暗号化したものである（図３から図５を用いて詳述する）。許諾側の計算機には、個別鍵生成２１、ソフト復号鍵２４、暗号化２３などを設ける。
【００４１】個別鍵生成２１は、ソフトウェア格納媒体１１から読み出した媒体固有番号１２をもとに媒体個別鍵を生成するものである（図６を用いて詳述する）。暗号化２３は、個別鍵生成２１によって生成された媒体個別鍵によって、ソフト復号鍵２４を暗号化するものである。この暗号化した暗号データは、ソフトウェア格納媒体１１に許諾情報１３として格納する。
【００４２】使用側の計算機には、個別鍵生成３１、復号３２、ソフト復号鍵３５、復号３４などを設ける。個別鍵生成３１は、ソフトウェア格納媒体１１から読み出した媒体固有番号１２をもとに媒体個別鍵を生成するものである（図６を用いて詳述する）。これは、許諾側の個別鍵生成２１と同じ、媒体個別鍵を生成する。
【００４３】復号３２は、個別鍵生成３１によって生成された媒体個別鍵により、ソフトウェア格納媒体１１から読み出した許諾情報１３を復号し、ソフト復号鍵３５を生成するものである（図８を用いて詳述する）。
【００４４】復号３４は、ソフト復号鍵３５によって、ソフトウェア格納媒体１１から読み出した暗号化ソフトウェア１５を復号し、平文のソフトウェアを生成するものである（図８を用いて詳述する）。この生成した平文のソフトウェアを実行する。
【００４５】以下図２の構成および動作を順次詳細に説明する。図３は、本発明のソフトウェア格納時のフローチャートを示す。これは、ソフトウェアを作成して暗号化した暗号化ソフトウェア１５および暗号化した許諾情報１３を、ソフトウェア格納媒体１１に格納する時のフローチャートである。
【００４６】図３において、Ｓ１は、ソフトウェアを作成する。これは、メーカがソフトウェア格納媒体に格納するソフトウェア（各種業務プログラム）を作成する。Ｓ２は、ソフトウェア暗号鍵の作成を行う。
【００４７】Ｓ３は、ソフトウェアに対応づけ、暗号鍵管理テーブルに格納する。これは、Ｓ１で作成したソフトウェアのソフトウェア名と、Ｓ２で作成した暗号鍵とを、例えば図５のソフトウェア暗号鍵管理テーブル４に図示のように対応づけて格納し、統括して管理する。
【００４８】Ｓ４は、指定したソフトウェアに対応したソフトウェア暗号鍵の取り出しを行う。これは、ソフトウェア格納媒体に格納するソフトウェア名に対応するソフトウェア暗号鍵を、図５のソフトウェア暗号鍵管理テーブル４から取り出す。
【００４９】Ｓ５は、Ｓ４で取り出したソフトウェア暗号鍵で、平文のソフトウェアを暗号化し、暗号化ソフトウェアを生成する。これは、例えば図４に示すように、作成したソフトウェア名とソフトウェア本体のうちソフトウェア本体の部分を、暗号化鍵によって暗号化を行い、図示のようにソフトウェア名と暗号化ソフトウェア本体を作成する。このときの暗号は、ＤＥＳなどを用い、下段に説明したように、換字とビット転置を繰り返して暗号化する。
【００５０】Ｓ６は、メーカ側の格納媒体に暗号化ソフトウェアを格納する。これにより、一度暗号化した暗号化ソフトウェアを保存し、次回以降は、この保存した暗号化ソフトウェアを取り出し、暗号化を省略する。
【００５１】Ｓ７は、暗号化ソフトウェアを読み込み、ソフトウェア格納媒体１１に格納する。Ｓ８は、ソフトウェア格納媒体１１に格納する暗号化ソフトウェアが終わったか判別する。ＹＥＳの場合には、終了する。ＮＯの場合には、Ｓ７を繰り返し行い、指示されたソフトウェア名の暗号化ソフトウェアをソフトウェア格納媒体１１に順次格納する。
【００５２】以上によって、ソフトウェアを作成してこれを暗号化した暗号化ソフトウェアにし、これをソフトウェア格納媒体１１に格納する。図４は、本発明のソフトウェアの暗号化の例を示す。
【００５３】図４の（ａ）は、ソフトウェアの暗号の様子を示す。ここで、ヘッダには、識別子としての役割を行うソフトウェア名などを格納する。このヘッダは、暗号化の対象としない。ソフトウェア本体は、暗号化の対象とし、暗号化鍵によって暗号化して暗号化ソフトウェア本体を作成する。このときの暗号化は、例えば図示の

ように、ＤＥＳ(Data Encryption Standard)を用いる。このＤＥＳは、換字とビット転置を繰り返し、暗号を行う。

【００５４】図4の（ｂ）は、暗号化の様子を示す。暗号化は、ＤＥＳによれば、図示のように６４ｂｉｔのビット列について、暗号化鍵によって暗号化を行い、同じ６４ｂｉｔのビット列を生成する。復号は、復号鍵によって元の６４ｂｉｔのビット列に復号する。

【００５５】図5は、本発明の暗号化ソフトウェアの格納例を示す。図5において、ソフトウェア暗号鍵管理テーブル4は、図3で既述したように、作成したソフトウェア名と、作成した暗号鍵とを対応づけて統括管理するテーブルである。このソフトウェア暗号鍵管理テーブル4には、ソフトウェアが暗号化されていることを表す“ＥＮＣ”を付与したソフトウェア名と、それぞれ６４ビットの暗号鍵をペアにして格納する。

【００５６】以下動作を説明する。

（１）ソフトウェア格納媒体に格納しようとする平文ソフトウェアについて、ソフトウェア暗号鍵管理テーブル4からソフトウェア暗号鍵を取り出す。

【００５７】（２）暗号化回路４１が渡されたソフトウェア暗号鍵によって、平文ソフトウェアを暗号化する。暗号化は、例えば図4のＤＥＳを用いて暗号化する。

【００５８】（３）暗号化した暗号化ソフトウェアをソフトウェア格納媒体１１に図示暗号化ソフトウェア１５として格納する。これを指定された全ての平文ソフトウェアについて終了するまで繰り返し行う。この際、一度、暗号化した暗号化ソフトウェアを保存すれば、次回以降からこの保存した暗号化ソフトウェアを取り出してソフトウェア格納媒体１１に格納すればよい。また、媒体固有番号１２は、既述したようにソフトウェア格納媒体１１に固有な一意な番号であって、書き替え不可の形で書き込まれている。また、ソフトウェア暗号鍵管理テーブル4に格納した暗号鍵は、暗号化のアルゴリズムに対象鍵番号を用いた場合には、復号鍵と当該暗号鍵とは一致する。

【００５９】以上によって、平文ソフトウェアについて、ソフトウェア暗号鍵管理テーブル4から該当するソフトウェア暗号鍵を取り出し、これを用いて暗号化を行って暗号化ソフトウェアを作成し、ソフトウェア格納媒体１１に格納する。

【００６０】図6は、本発明の許諾情報の生成フローチャートを示す。これは、許諾しようとするソフトウェアの暗号化した許諾情報１３を生成し、ソフトウェア格納媒体１１に格納するフローチャートである。

【００６１】図6において、Ｓ１１は、許諾しようとするソフトウェア名を入力する。Ｓ１２は、復号鍵管理テーブル5より、ソフト復号鍵を取り出す。これは、図7のソフトウェア復号鍵管理テーブル5から許諾を与えようとするソフトウェア名の復号鍵を取り出す。

【００６２】Ｓ１３は、媒体固有番号の取り出しを行う。これは、許諾情報を書き込もうとする、ソフトウェア格納媒体１１の媒体固有番号を読み出す。Ｓ１４は、媒体個別鍵の生成を行う。これは、右側に記載したように、ソフトウェア格納媒体１１から読み出した平文の媒体固有番号１２について、秘密鍵によって暗号化した媒体個別鍵を生成したり、あるいは平文の媒体固有番号１２について、秘密アルゴリズムによって暗号化した媒体個別鍵を生成したりする。

【００６３】Ｓ１５は、媒体個別鍵によって、ソフト復号鍵を暗号化し、許諾情報を生成する。これは、右側に記載したように、平文のソフト復号鍵について、Ｓ１４で生成した媒体個別鍵により暗号化し、許諾情報を生成する。

【００６４】Ｓ１６は、Ｓ１５で生成した暗号化した許諾情報をソフトウェア格納媒体１１に格納する。

【００６５】以上によって、暗号化ソフトウェア１５を格納したソフトウェア格納媒体１１から媒体固有番号１２を読み出して媒体個別鍵を生成し、ソフト復号鍵についてこの媒体個別鍵で暗号化し、暗号化した許諾情報１３を生成してフトウェア格納媒体１１に格納する。これにより、暗号化ソフトウェア１５および暗号化した許諾情報１３をソフトウェア格納媒体１１に格納したこととなる。

【００６６】図7は、本発明の許諾情報の生成説明図を示す。図7において、ソフトウェア復号鍵管理テーブル5は、暗号化ソフトウェア１５を復号して平文のソフトウェアに復号する際に必要なソフト復号鍵を、ソフトウエァ名に対応づけて管理するものである。このソフトウェア復号鍵管理テーブル5には、図5で説明したソフトウェア暗号鍵管理テーブル4と同様の復号鍵を格納する。ここには、暗号化されていることを表す“ＥＮＣ”を付与したソフトウェア名と、それぞれのソフトウェアに対応して６４ビットのソフト復号鍵をペアに格納する。動作を説明する。

【００６７】（１）許諾情報を使用側に販売する場合、まず、ソフトウェア格納媒体１１から媒体固有番号１２を読み出す。この読み出した媒体固有番号１２を個別鍵生成回路２１１に入力し、媒体個別鍵を生成する（図6のＳ１４参照）。

【００６８】（２）次に、販売しようとするソフトウェアのソフト復号鍵をソフトウェア復号鍵管理テーブル5から取り出して暗号化回路２３１に入力し、媒体個別鍵で暗号化し、図示許諾情報１３を生成する。この許諾情報１３は、ＥＮＣという暗号化した旨を表す識別子を付与したソフトウェア名と、暗号化した許諾情報とをペアにし、ソフトウェア格納媒体１１に許諾情報１３として格納する。ここで、ソフトウェア復号鍵と、個別鍵生成回路２１１のアルゴリズム（あるいは秘密鍵）は、安全な手段によって保護する。

【0069】以上によって、許諾側は、ソフトウェア格納媒体11から読み出した媒体固有番号12をもとに媒体個別鍵を生成し、この媒体個別鍵をもとに、ソフト復号鍵を暗号化してソフトウェア格納媒体11に許諾情報13として格納する。

【0070】図8は、本発明のソフトウェア復号のフローチャートを示す。これは、使用側が購入したソフトウェア格納媒体11を計算機に装着し、ソフトウェアを主記憶にローディングして実行するときのフローチャートである。

【0071】図8において、S21は、ソフトウェアの実行命令を受け取る。S22は、ソフトウェア格納媒体11から媒体固有番号12の取り出しを行う。

【0072】S23は、媒体個別鍵の生成を行う。これは、右側に記載したように、S22でソフトウェア格納媒体11から取り出した媒体固有番号12について、秘密鍵により暗号化した媒体個別鍵を生成する。あるいは秘密アルゴリズムにより、媒体固有番号12から暗号化した媒体個別鍵を生成する。

【0073】S24は、S23で生成した媒体個別鍵で、ソフトウェア格納媒体11から読み出した許諾情報13を復号し、ソフト復号鍵を生成する。これは、右側に記載したように、S23で暗号化した媒体個別鍵で、暗号文である許諾情報13を復号化して平文のソフト復号鍵35を生成する。

【0074】S25は、ソフトウェア格納媒体11から暗号化ソフトウェア15の読み込みを行う。S26は、ソフト復号鍵で、S25で読み込んだ暗号化ソフトウェア15を復号し、平文のソフトウェアを生成する。これは、右側に記載したように、暗号文の暗号化ソフトウェア15について、S24で生成したソフト復号鍵35で復号し、平文のソフトウェアを生成する。S27は、ソフトウェア実行する。

【0075】以上によって、ソフトウェア実行命令に対応して、ソフトウェア格納媒体11から取り出した媒体固有番号12から媒体個別鍵を生成し、この媒体個別鍵をもとにソフトウェア格納媒体11から取り出した許諾情報13を復元してソフト復号鍵35を生成し、このソフト復号鍵35によって、ソフトウェア格納媒体11から取り出した暗号化ソフトウェア15を復号して平文のソフトウェアを生成する。この平文のソフトウェアを主記憶にローディングし、実行することが可能となる。

【0076】図9は、本発明のプログラムの場合の説明図を示す。これは、電子化データとしてプログラムの場合の説明図である。図9の（a）は、全体構成図を示す。

【0077】図9の（a）において、光磁気ディスク6は、暗号化プログラムなどを格納するものであって、図2のソフトウェア格納媒体11に対応するものであり、媒体固有番号12、許諾情報13、および暗号化プログラム16を格納する媒体である。この光磁気ディスク6は、許諾側から購入し、光磁気ディスク装置に装着する。この光磁気ディスク6の他に、光ディスク、CD-ROM、FD、HD、磁気テープ、カセットテープなどの記憶媒体であってもよい。

【0078】プログラムローダ61は、プログラム命令実行時に、光磁気ディスク6から該当する復号したプログラムを主記憶63にローディングし、実行可能な状態にするものであって、ここでは、既述した鍵生成（個別鍵生成31）、復号（復号32、34）などを備えた処理部である。

【0079】主記憶63は、プログラムローダ61が光磁気ディスク6から取り出して復号した平文のプログラムを展開するためのRAM（読み書き可能なメモリ）である。

【0080】次に、図9の（b）のフローチャートに示す順序に従い、図9の（a）の構成の動作を説明する。図9の（b）において、S31は、プログラム命令実行を受け取る。

【0081】S32は、プログラムローダ61が実行プログラムを見つけて取り出し、復号する。S33は、主記憶上にメモリ展開する。これは、S32で復号した平文のプログラムを、主記憶63上に展開し、動作可能な状態にする。

【0082】S34は、プログラム実行する。S33で主記憶63上に展開された平文のプロウラムを実行する。図9の（c）は、ユーザ計算機でのソフトウェア（プログラム）の実行説明図を示す。

【0083】（1）ユーザ計算機がソフトウェア格納媒体11から媒体固有番号12を取り出して個別鍵生成回路311に入力し、暗号化した媒体個別鍵を生成する（図8のS23参照）。

【0084】（2）復号回路321が、ソフトウェア格納媒体11から取り出した図示のような許諾情報13について、（1）で生成した媒体個別鍵により復号し、図示のようなソフトウェア復号鍵351（ソフト復号鍵35に対応する）を生成する。

【0085】（3）復号回路341が、ソフトウェア格納媒体11から取り出した暗号化ソフトウェア15について、（2）で生成したソフトウェア復号鍵351により復号し、平文のソフトウェア（プログラム）を生成する。この平文のソフトウェア（プログラム）を主記憶63に展開し、実行する。

【0086】ここで、許諾情報13が格納されていない暗号化ソフトウェア15は復号することができず、実行不可能である。また、ソフトウェア格納媒体11を他の媒体の不正にコピーした場合には、媒体固有番号12が無い、あるいは異なるため、許諾情報13から正しいソフトウェア復号鍵351を復号できず、結果として暗号化ソフトウェアを平文のソフトウェアに復号できず、実

行不可能である。尚、ユーザ計算機上では、個別鍵生成回路３１１のアルゴリズムあるいは秘密鍵、生成したソフトウェア復号鍵、復号した平文ソフトウェアは安全な手段によって保護する。

【００８７】図１０は、本発明のデータの場合の説明図を示す。これは、電子化データとしてデータ、例えば出版物などの文字データ（テキスト）、記号、画像データ、更に音声データなどの場合の説明図である。

【００８８】図１０の（ａ）は、全体構成図を示す。図１０の（ａ）において、光磁気ディスク６は、暗号化データなどを格納するものであって、図２のソフトウェア格納媒体１１に対応するものであり、媒体固有番号１２、許諾情報１３、および暗号化データ１７を格納する媒体である。この光磁気ディスク６は、許諾側から購入し、光磁気ディスク装置に装着する。この光磁気ディスク６の他に、光ディスク、ＣＤ－ＲＯＭ、ＦＤ、ＨＤ、磁気テープ、カセットテープなどの記憶媒体であってもよい。

【００８９】Ｒ／Ｗモジュール６４は、リード命令実行時に、光磁気ディスク６から該当する復号したデータを主記憶６３に格納するものであって、ここでは、既述した鍵生成（個別鍵生成３１）、復号（復号３２、３４）などを備えた処理部である。

【００９０】主記憶６３は、Ｒ／Ｗモジュール６４が光磁気ディスク６から取り出して復号した平文のデータを格納するためのＲＡＭ（読み書き可能なメモリ）である。次に、図１０の（ｂ）のフローチャートに示す順序に従い、図１０の（ａ）の構成の動作を説明する。

【００９１】図１０の（ｂ）において、Ｓ４１は、アプリケーション実行する。Ｓ４２はデータ読み込み命令を実行する。Ｓ４３は、Ｒ／Ｗモジュール６４がデータを見つけ、読み込み復号する。Ｓ４４は、主記憶上に格納する。Ｓ４５は、データの表示、再生を行う。

【００９２】以上によって、Ｓ４２でデータの読み込み命令があったときに、Ｒ／Ｗモジュール６４が、光磁気ディスク６から暗号化データ１７を取り出して復号して平文のデータを生成し、これを主記憶６３に格納する。そして、主記憶６３から取り出してディスプレイ上に出版物の文字列として表示したり、画像を表示したり、音声として発生したりする。次に、Ｒ／Ｗモジュール６４の動作を詳細に説明する。

【００９３】図１０の（ｃ）は、ユーザ計算機でのデータの表示／再生説明図を示す。

（１）ユーザ計算機がデータ格納媒体１１１から媒体固有番号１２を取り出して個別鍵生成回路３１１に入力し、暗号化して媒体個別鍵を生成する（図８のＳ２３参照）。

【００９４】（２）復号回路３２１が、データ格納媒体１１１から取り出した図示のような許諾情報１３について、（１）で生成した媒体個別鍵により復号し、図示のようなデータ復号鍵３５２（ソフト復号鍵３５に対応する）を生成する。

【００９５】（３）復号回路３４１が、データ格納媒体１１１から取り出した暗号化データ１７について、（２）で生成したデータ復号鍵３５２により復号し、平文のデータ（文字データ、画像データ、音声データなど）を生成する。この平文のデータを主記憶６３に格納し、ディスプレイ上に出版物の文字列、画像、記号として表示したり、音声として発生したりする。

【００９６】図１１は、ＲＯＭ／ＲＡＭ混在型光磁気ディスクに適用した場合を示す。ＲＯＭ／ＲＡＭ混在型の光磁気ディスクは、図示のように、ユーザ書換え不可能な領域、読み書き可能領域、読み出し専用領域／読み書き専用領域がある。従って、これら領域に図示のように媒体固有番号１２、許諾情報１３、暗号化ソフトウェア１５を格納する。これにより、ユーザ書換え不可能な領域に、媒体固有番号１２を書き込むため、当該光磁気ディスクの固有な媒体固有番号を与え、本発明の保護を図ることができる。

【００９７】図１２は、本発明の許諾情報を他の格納媒体に格納する場合の例を示す。この場合には、図示のように、ソフトウェア格納媒体に固有な一意の媒体固有番号と、暗号化ソフトウェアのみを予め格納する。そして、許諾情報を別の許諾情報格納媒体に格納する。これは、ＣＤ－ＲＯＭなどの書き込む領域を持たない媒体に媒体固有番号および暗号化ソフトウェア（暗号化データ）を予め書き込んでおき、当該ＣＤ－ＲＯＭなどのうちの許諾を与える許諾情報を別の書き込み可能な許諾情報格納媒体（例えばＦＬＯＰＰＹ（登録商標）など）に書き込む場合の実施例である。

【００９８】図１３は、本発明の複数のソフトを１枚の媒体に格納する場合の説明図を示す。これは、複数のソフト（あるいはデータ）を１枚の大容量の媒体（光磁気ディスク、ＣＤ－ＲＯＭなど）に格納し、個別販売する場合の実施例である。この場合には、ソフト復号鍵１、２・・・Ｎについて、それぞれ媒体固有鍵によって暗号化した許諾情報１、２・・・Ｎを生成してソフトウェア格納媒体１１に格納する。そして、ユーザは、ソフトウェア格納媒体１１に格納されている暗号化ソフト１、２・・・Ｎのうち、購入希望のソフトウェア名を許諾情報販売側に通知すると、許諾情報販売側はソフトウェアに対応するソフト復号鍵を媒体固有番号から生成した媒体個別鍵で暗号化し、これを許諾情報としてソフトウェア格納媒体１１に格納する。ユーザは、このソフトウェア格納媒体１１を装着し、購入した暗号化ソフトウェアを復号して平文のソフトウェアにし、使用する。一方、ユーザは、許諾情報のないソフトウェアを利用しようとしても暗号化ソフトウェアを復号できず、使用できない。また、他のソフトウェア格納媒体１１の許諾情報をコピーしても、ソフトウェア格納媒体１１の媒体固有番号が

コピーできないため、正しい復号ができない。これにより、ソフトウェアの個別販売を行うことが可能となる。

【0099】

【発明の効果】以上説明したように、請求項1の発明によれば、記憶媒体を一意に特定する媒体固有番号に基づいてデータを暗号化し、暗号化した暗号化データを記録媒体に書き込むよう構成したので、媒体固有番号に基づく暗号化を伴った暗号化データの書き込みをおこなうことが可能なデータ書込装置が得られるという効果を奏する。

【0100】また、請求項2の発明によれば、暗号化データを読み取るデータ読取装置による書き替えが不可能な形式で媒体固有番号を記憶媒体に記憶するよう構成したので、記憶媒体に記憶した暗号化データを他の記憶媒体に複写する不正使用を防止することが可能なデータ書込装置が得られるという効果を奏する。

【0101】また、請求項3の発明によれば、記憶媒体から媒体固有番号を読み取り、読み取った媒体固有番号に基づいて、記憶媒体上の暗号化データを復号するよう構成したので、正規な記憶媒体に記憶された暗号化データのみを正しく復号化し、もってデータの不正使用を効率良く防止することが可能なデータ読取装置が得られるという効果を奏する。

【0102】また、請求項4の発明によれば、記憶媒体は、データ読取装置による書き替えが不可能な形式で媒体記憶番号を記憶するよう構成したので、記憶媒体に記憶した暗号化電子化データを他の記憶媒体に複写する不正使用を防止することが可能なデータ読取装置が得られるという効果を奏する。

【0103】また、請求項5の発明によれば、各記憶媒体を一意に特定する媒体固有番号と、媒体固有番号に基づいて暗号化した暗号化データとを記憶媒体に格納するよう構成したので、媒体固有番号を利用して暗号化した暗号化データを簡易に授受することが可能な記憶媒体が得られるという効果を奏する。

【0104】また、請求項6の発明によれば、データ書込装置によって暗号化データを生成するために使用される媒体固有番号を格納するよう構成したので、かかる媒体固有番号を用いて効率良く暗号化することが可能な記憶媒体が得られるという効果を奏する。

【0105】また、請求項7の発明によれば、データ読取装置によって暗号化データを復号するために使用される媒体固有番号を格納するよう構成したので、かかる媒体固有番号を用いて効率良く復号化することが可能な記憶媒体が得られるという効果を奏する。

【0106】また、請求項8の発明によれば、データ読取装置による書き替えが不可能な形式で媒体記憶番号を記憶するよう構成したので、記憶媒体に記憶した暗号化データを他の記憶媒体に複写する不正使用を防止することが可能な記憶媒体が得られるという効果を奏する。

【0107】また、請求項9の発明によれば、記憶媒体に格納された該記憶媒体を一意に特定する媒体固有番号を読み取り、読み取った媒体固有番号に基づいて媒体固有鍵を生成するよう構成したので、データ書込装置とデータ読取装置が容易に鍵を共有化することが可能な鍵共有方法が得られるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

【図2】本発明の1実施例構成図である。

【図3】本発明のソフトウェア格納時のフローチャートである。

【図4】本発明のソフトウェアの暗号化の例である。

【図5】本発明の暗号化ソフトウェアの格納例である。

【図6】本発明の許諾情報の生成フローチャートである。

【図7】本発明の許諾情報の生成説明図である。

【図8】本発明のソフトウェア復号のフローチャートである。

【図9】本発明のプログラムの場合の説明図である。

【図10】本発明のデータの場合の説明図である。

【図11】ROM／RAM混在型光磁気ディスクに適用した場合である。

【図12】本発明の許諾情報を他の格納媒体に格納する場合の例である。

【図13】本発明の複数ソフトを1枚の媒体に格納する場合の説明図である。

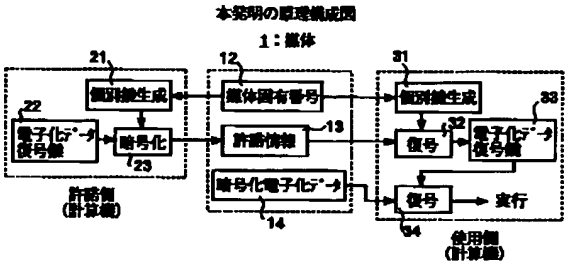
【図14】従来技術の説明図である。

【符号の説明】

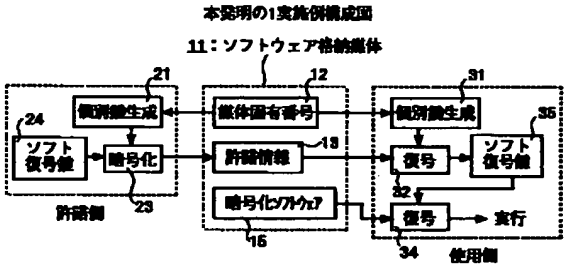
1：媒体
11：ソフトウェア格納媒体
111：データ格納媒体
12：媒体固有番号
13：許諾情報
14：暗号化電子化データ
15：暗号化ソフトウェア
16：暗号化プログラム
17：暗号化データ
21：個別鍵生成
211：個別鍵生成回路
22：電子化データ復号鍵
23：暗号化
231：暗号化回路
24：ソフト復号鍵
31：個別鍵生成
311：個別鍵生成回路
32：復号
321：復号回路
33：電子化データ復号鍵
34：復号
341：復号回路

35：ソフト復号鍵
351：ソフトウェア復号鍵
352：データ復号鍵
41：暗号化回路
6：光磁気ディスク
61：プログラムローダ
63：主記憶
64：R／Wモジュール

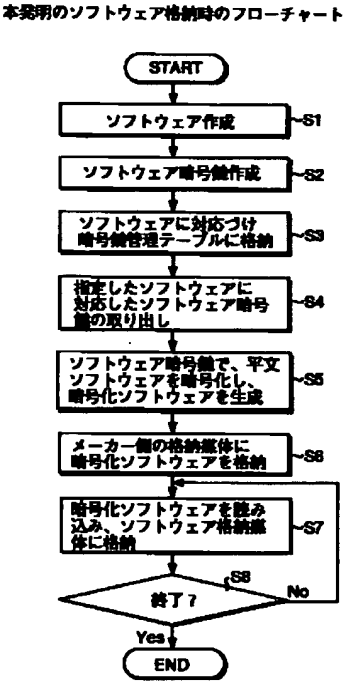
【図1】



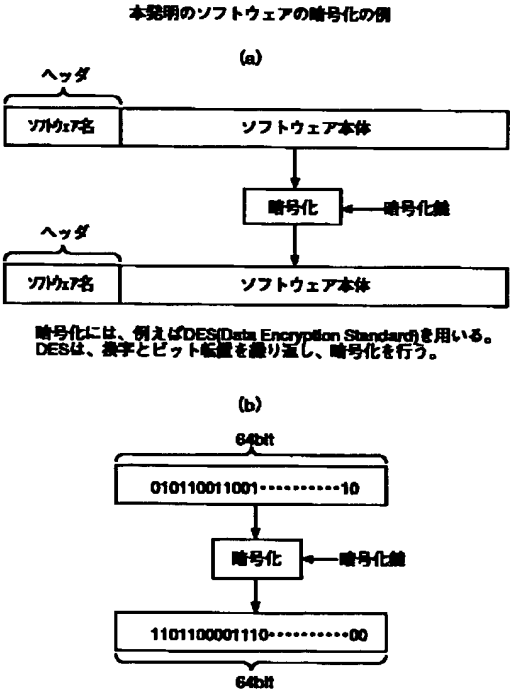
【図2】



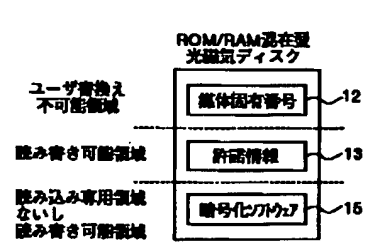
【図3】



【図4】

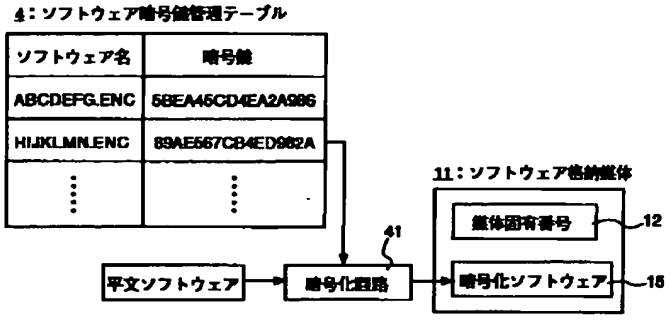


【図11】



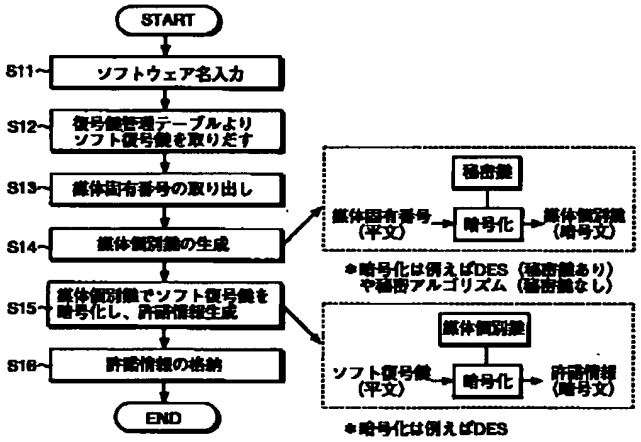
【図5】

本発明の暗号化ソフトウェアの格納例



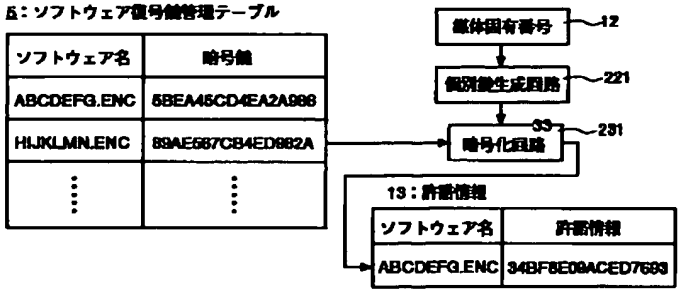
【図6】

本発明の許諾情報の生成フローチャート

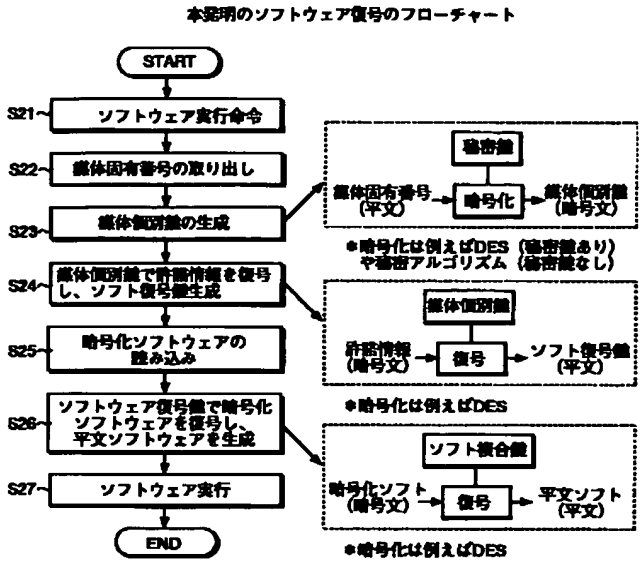


【図7】

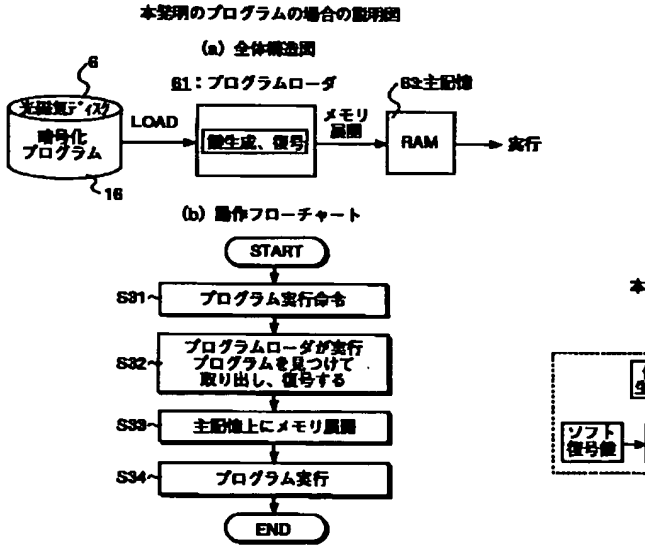
本発明の許諾情報の生成説明図



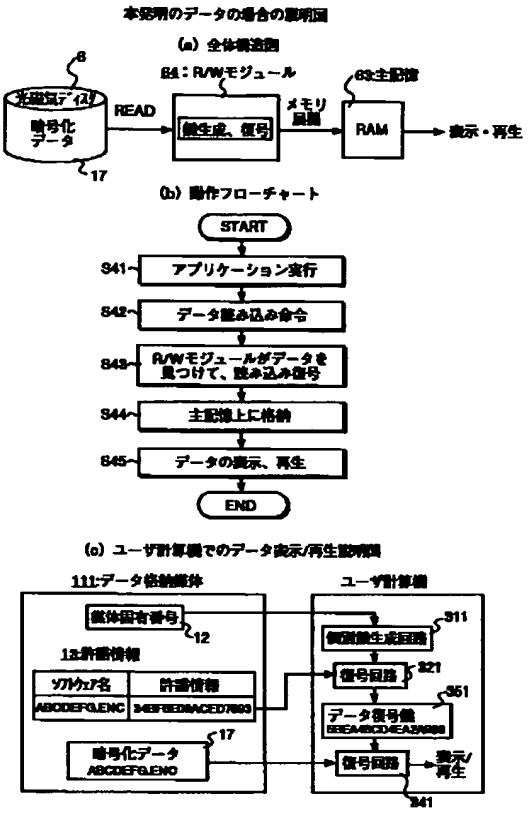
【図8】


本発明のソフトウェア復号のフローチャート
START
S21 ソフトウェア実行命令
S22 媒体固有番号の取り出し
S23 媒体個別鍵の生成
S24 媒体個別鍵で許諾情報を復号し、ソフト復号鍵生成
S25 暗号化ソフトウェアの読み込み
S26 ソフトウェア復号鍵で暗号化ソフトウェアを復号し、平文ソフトウェアを生成
S27 ソフトウェア実行
END
秘密鍵
媒体固有番号（平文）
暗号化
媒体個別鍵（暗号文）
＊暗号化は例えばDES（秘密鍵あり）や秘密アルゴリズム（秘密鍵なし）
媒体個別鍵
許諾情報（暗号文）
復号
ソフト復号鍵（平文）
＊暗号化は例えばDES
ソフト復合鍵
暗号化ソフト（暗号文）
復号
平文ソフト（平文）
＊暗号化は例えばDES

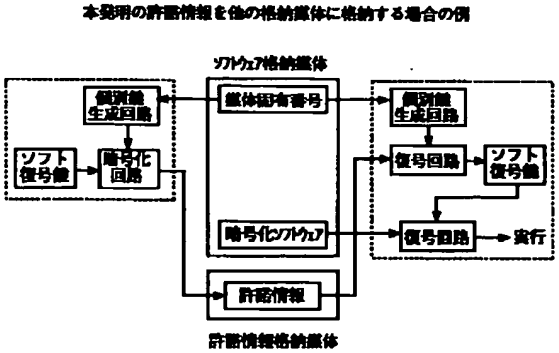
【図9】


本発明のプログラムの場合の説明図
(a) 全体構造図
6
光磁気ディスク
暗号化プログラム
16
LOAD
61：プログラムローダ
鍵生成、復号
メモリ展開
63:主記憶
RAM
実行
(b) 動作フローチャート
START
S31 プログラム実行命令
S32 プログラムローダが実行プログラムを見つけて取り出し、復号する
S33 主記憶上にメモリ展開
S34 プログラム実行
END
(c) ユーザ計算機でのソフトウェアの実行説明図
11:ソフトウェア格納媒体
ユーザ計算機
媒体固有番号
12
12:許諾情報
ソフトウェア名
許諾情報
ABCDEFG.ENC
暗号化ソフトウェア
ABCDEFG.ENC
15
個別鍵生成回路
311
復号回路
321
ソフトウェア復号鍵
351
復号回路
実行
341

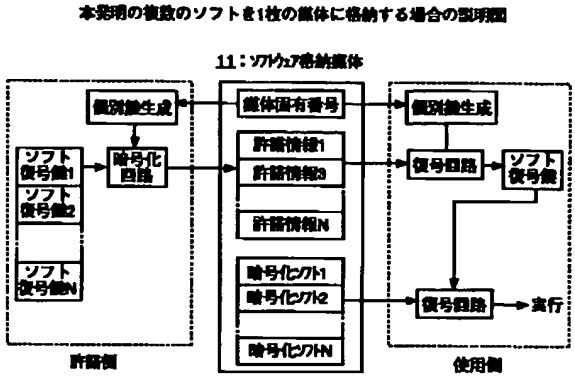
【図10】


本発明のデータの場合の説明図
(a) 全体構造図
6
光磁気ディスク
暗号化データ
17
64：R/Wモジュール
READ
鍵生成、復号
メモリ展開
63:主記憶
RAM
表示・再生
(b) 動作フローチャート
START
S41 アプリケーション実行
S42 データ読み込み命令
S43 R/Wモジュールがデータを見つけて、読み込み復号
S44 主記憶上に格納
S45 データの表示、再生
END
(c) ユーザ計算機でのデータ表示/再生説明図
111:データ格納媒体
ユーザ計算機
媒体固有番号
12
12:許諾情報
ソフトウェア名
許諾情報
ABCDEFG.ENC
暗号化データ
ABCDEFG.ENC
17
個別鍵生成回路
311
復号回路
321
データ復号鍵
351
復号回路
表示/再生
341

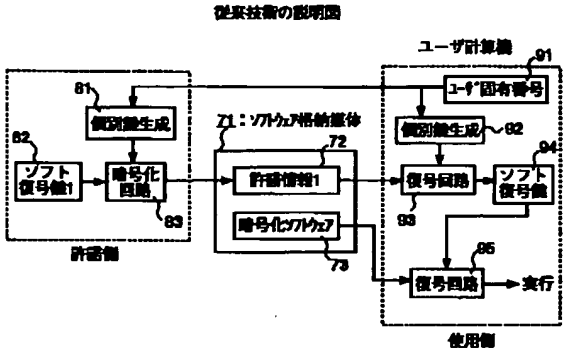
【図12】


本発明の許諾情報を他の格納媒体に格納する場合の例
ソフトウェア格納媒体
個別鍵生成回路
ソフト復号鍵
暗号化回路
媒体固有番号
暗号化ソフトウェア
許諾情報
個別鍵生成回路
復号回路
ソフト復号鍵
復号回路
実行
許諾情報格納媒体

【図13】



【図14】



フロントページの続き

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内

PAT-NO: JP02000315175A
DOCUMENT-IDENTIFIER: JP 2000315175 A
TITLE: DATA WRITER, DATA READER, STORAGE MEDIUM AND KEY SHARING METHOD
PUBN-DATE: November 14, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
HASEBE, TAKAYUKI	N/A
AKIYAMA, RYOTA	N/A
YOSHIOKA, MAKOTO	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
FUJITSU LTD	N/A

APPL-NO: JP2000079015
APPL-DATE: March 16, 1992

INT-CL (IPC): G06F012/14 , G06F009/06 , H04L009/08

ABSTRACT:

PROBLEM TO BE SOLVED: To allocate a medium inherent number to a medium, to provide license to execute software to the inherent number and to make it possible to execute only the software licensed and stored in a normal medium.

SOLUTION: Ciphered electronic data 14 and a medium inherent number 12 inherent in a medium 1 are stored in the medium 1. A licenser side generates a medium inherent key on the basis of the inherent number 12 of the medium 1 and ciphers an electronic data deciphering key as license information 13 by using the medium inherent key and a user side generates a medium inherent key based on the medium inherent number 12 read out from the medium 1, deciphers the license information 13 by using the medium inherent key and deciphers the read ciphered electronic data 14 by the electronic data deciphering key to obtain normal electronic data.